REMARKS:

Claims 1, 30 and 31 are objected to because in claim 1 the second paragraph reads "for storing response". Applicant has corrected this phrase to read "for storing a response".

Claims 30 and 31 have been corrected to properly refer to the method of claim 22.

Claims 1-3, 6-7, 9, 10-12, 15, 16, and 17-31 are rejected under 35 USC § 101 because the claimed invention is directed to non-statutory subject matter. Respectfully, these claims have been present in this application since it was filed in December 2001. The present office action is the fourth office action on this application. The claims have not changed significantly since filed and applicant respectfully submits that if the rejection were proper, which it is not, it should have been made years ago.

Turning to the rejection, the invention relates to apparatus that is implemented in hardware and software in a manner that is clearly statutory. Turning to claim 1 for example, the claim recites <u>apparatus</u> for connecting a machine to a central system by way of a public network. The claim includes two specific hardware elements, a message generator and a receiver. Even if the message generator and receiver are implemented as software controlled hardware elements, they are clearly statutory. The examiner has offered no authority for the rejection. The suggestion to add a memory for storing messages actually answers the rejection. The claim includes a receiver for receiving and storing a response. A receiver is clearly a hardware element even

if controlled by software. It is characterized as having the capability for receiving and storing a response and therefore it implicitly includes memory for carrying out the storing even though memory isn't separately recited. Applicant respectfully requests that this aspect of the rejection be withdrawn.

Claims 1-9 are rejected as failing to comply with the enablement requirement. As was the case with the rejection under section 101, this rejection relates to claims that have been present in the application for over four years and have been the subject of four office actions. The examiner objects to the limitation "a message generator for creating an application layer message document including a unique machine name and password combination in a format suitable for transmission over a network". The examiner acknowledges that applicant's written description specifically discusses providing security through credentials such as a user ID and password and through authentication tokens. It appears to be the essence of the rejection that use of a password to identify a machine is not well known in the art. The examiner notes that the use of an identifier and password is typically reserved for authenticating users not machines. Applicant respectfully submits that the fact that applicant is using an identifier and password to authenticate a machine not a user does not support the examiner's assertion that it would require undue experimentation for one of ordinary skill in the art at the time the invention was made to determine how to use a unique name and password to authenticate a machine. Applicant submits that it is the conception of the idea to use a unique machine name and password to authenticate a machine that is the important aspect of the invention, not the implementation which applicant submits would not only require no undue experimentation but no experimentation at all. The use of

unique names and passwords for users has been known for 30 years or more. Only applicant's suggestion to apply the same technique to a machine would be necessary for one of ordinary skill in the art to understand how to implement the invention. The examiner has identified nothing about applicant's invention that is difficult to implement. The fact that no one has ever though about using an identifier and password for a machine rather than a user doesn't change the fact that the implementation would be well within the abilities of one of ordinary skill in the art.

Claims 1-9 are also rejected under 35 USC § 112 second paragraph as being indefinite. The examiner asserts that applicant's claim limitation of "a message generator for creating an application layer message document including a unique machine name and password combination in a format suitable for transmission over a network" is using terms contrary to their ordinary meaning in the art. To the contrary, as explained above, applicant is using an identifier/password combination exactly as the term would be understood by one of ordinary skill in the art. The fact that no one prior to applicant has used such a combination to authenticate a machine doesn't change the fact that the terms are well understood. The examiner's supposition that applicant is intending to use the term "machine name and password" to broadly cover known authentication methods is wrong. Applicant uses the terms in a conventional sense as would be well understood by those skilled in the art.

The examiner's suggestion that the limitation be re-written as a "unique machine name and information for authenticating and authorizing each machine" is hardly different. Applicant's claim is more specific in that the

"information" suggested by the examiner is a password as claimed by applicant. Note also that the claim requires that the name and password combination be included in an application layer message document in hypertext format. This further limits the claim and adds no indefiniteness.

Claim 6 has been amended to clarify the fact that the message is the message document thereby providing clear antecedent basis.

Claims 1-9 are rejected under 35 U.S.C. 102(e) as anticipated by Tabbara (US Patent Application Publication 2005/01/02388).

First, applicant notes that the publication is a continuation of application serial number 09/695,820 now patent number 6,886,038. Applicant questions why the examiner relied on the publication not the patent. The examiner has made no showing that the disclosure of the original application is the same as the published application thereby entitling the publication to an earlier filing date. Use of the patent would have avoided this problem.

Referring first to Tabbara, the publication relates to an invention for restricting data transfers and managing software components in clusters of server computers located at a co-location facility (paragraph 11). It does not relate in any way to connecting machines other than computers to a network or for managing or servicing machines other than computers.

Claim 1 relates to apparatus for connecting a remote machine to a central system. The remote machine includes a message generator for creating an application layer message document including a unique machine name and password combination in hypertext format. The examiner points to paragraphs 27 and 88 of Tabbara. Page 27 refers only to communication between client

computers 102 and server computers in clusters 106. While admittedly these computers communicate with one another using the hypertext transfer protocol HTTP, there is nothing else in Tabbara that suggests that the client computers are anything other than web browsers. In fact, this is the essence of Tabbara.

Claim 1 requires more. The claim relates to apparatus for connecting a remote machine to a central system. Nothing in Tabbara suggests that the client computers are either the remote machines or that the computers could be connected to a remote machine as required by claim 1.

Paragraphs 3-9 describe the background of the invention and the use of clusters of computers to provide web pages to clients. Nowhere is there any suggestion that the client computers or any other computers of Tabbara are connected to machines.

Moreover, paragraph 88 describes ownership domains that include a public key and a storage key. What is missing however is any discussion of how an ownership domain corresponds to a client computer. For example, figure 6 shows a block diagram of an exemplary set of ownership domains. As described in paragraph 82, the ownership domains apparently exist only in BMonitor 250 (see figure 5). As described in paragraph 59, node 248 that includes BMonitor 250 can be a node of a co-location facility or alternatively a separate device for example a client or server. Node 248 includes BMonitor 250 and the plurality of software components or engines 252. As described at paragraph 60, node 248 may include multiple processors for executing engines 252 and another processor to execute BMonitor 250. Only software can be "executed". Clearly, BMonitor is software.

Claim 1 requires that a message generator create an application layer message document including a unique machine name and password combination in hypertext format. The examiner has not pointed to anything in Tabbara that suggests a unique machine name and password. The examiner has attempted to change applicant's unique machine name and password to a machine name and information for authenticating and authorizing each machine but that is not what applicant claims. Even if the examiner's language were accepted as being equivalent to the scope of applicant's claim, what paragraph 82 says is that the BMonitor operates as a trusted third party mediating interaction among multiple mutually distrustful management agents that share responsibility for managing node 248. Thus it is BMonitor that is trusted and if there is information for authenticating and authorizing anything it is information for authenticating and authorizing the trusted BMonitor not the machine name and password claimed by applicant.

Furthermore, Claim 1 requires a message generator subsequently creating messages using the unique machine name and password. There is nothing in Tabbara that suggests that the BMonitor does this. All the examiner suggests is that Tabbara discloses a private key pair. Referring to paragraph 89, pointed to by the examiner, the BMonitor generates a token which Tabbara describes as a random number and encrypts the token and sends it to the requesting management device. The management device decrypts the token and returns the decrypted token to BMonitor 250. Tabbara never suggests that even if the token is equivalent to a unique machine name and password, which it isn't because it is described as no more than a random number, creating messages using the token.

13

With regard to Claims 2 or 3, at this time applicant doesn't separately argue the patentability of Claims 2 or 3.

With regard to Claim 4, the examiner points to paragraph 35 but no where in paragraph 35 is there any mention of a gateway device that provides protocol or address translation.

With regard to Claim 5, the claim requires memory in the central system for storing the unique name and password and information identifying the type of machine. The examiner points to paragraph 88 and 89 of Tabbara but neither of these paragraphs mentions a unique machine name and password and neither of these paragraphs mentions storing information identifying the type of machine. Paragraph 88 describes each ownership domain including an identifier, a public key and a storage key. There is no mention of storing information identifying a type of machine. Paragraph 89 talks only about authenticating management devices to tokens as already discussed. There is no suggestion to store a unique name and password or storing information identifying a type of machine. Since Tabbara is only concerned with authentication, there would be no need to store information identifying a type of machine.

With regard to Claim 6, applicant doesn't separately argue the patentability of Claim 6 at this time.

With regard to Claim 7, the claim requires that the registration message includes identifying information, information on the type of machine, network address and accessibility. The examiner points to paragraphs 85 and 86. Paragraph 85 describes rights possessed by an ownership domain. It does not

14

suggest that those rights would be included in a registration message, and in fact does not mention a registration message at all. Furthermore, none of the rights listed shows or suggests providing information on the type of machine.

As to network address the examiner notes that all TCP/IP messages inherently include an address. What the examiner fails to note is that the claim relates to an address in an application layer message document in hypertext format. To the extent that all TCP/IP messages include an address, the address is in binary format and is not included in an application layer message document in hypertext format. Nothing in the paragraphs referred to by the examiner suggests anything else.

With regard to Claim 8, the claim requires memory for storing a token indicating that the machine is registered and inhibiting subsequent sending of registration messages. The examiner points to paragraph 88 of Tabbara. Even if Tabbara describes a registration message which applicant does not admit for the reasons already discussed, nothing in paragraph 88 suggests inhibiting subsequent sending of registration messages. In fact, the contrary is the case. Paragraph 88 specifically provides that each time a new ownership domain is created the ownership domain that creates the ownership domain communicates an ID and a public key to BMonitor 250 for the new ownership domain. This is contrary to applicant's suggestion that once a machine is registered further registration messages are inhibited.

With respect to Claim 9, the claim requires that the registration message includes a non-unique identifier and a response includes a unique identifier to be used by the machine in subsequent messages. The examiner points to paragraph 88 but it is clear that the ownership domain includes an identifier, a

15

public key and a storage key. Tabbara specifically states "the identifier serves as a unique identifier of the ownership domain,". Nothing in Tabbara suggests that a non-unique identifier be used to trigger a response from a server that includes a unique identifier. In fact the contrary is the case since it is the essence of the BMonitor to authenticate domains not known to be trustworthy and non-unique identifiers could not be used to do this.

Claims 10 and 13-31 are rejected as anticipated by Bush (U.S. 6,754,664).

Claim 10 relates to apparatus for connecting a remote machine to a central system. Unlike Tabbara, Bush at least generally relates to such an arrangement. However, the apparatus described in claim 10 is intended to overcome a particular problem created by the widespread use of network address translation and the accompanying inability of central systems to initiate connections to remote machines. This problem arises because machines located behind a firewall that have local addresses only can't be reached from the outside. They can initiate connections with central servers but the reverse is not true. Once a machine behind a firewall initiates a connection, the connection is two way and information can pass in both directions until the connection is broken. Claim 10 addresses this problem by periodically activating a message generator in the remote machine according to a stored schedule and then activating a receiver for a predetermined time after the message generator is activated for receiving messages from the central server. In this way, if the central server has a message for the remote machine it can be received on schedule by way of a connection created by the remote machine which has no way of knowing that a message is waiting for it.

16

With this in mind we turn to the limitations of claim 10. Claim 10 requires a message generator for sending a registration message to a central system from the remote machine, the registration message including a unique identifier. A schedule is stored and used to periodically activate the message generator according to the stored schedule. A receiver is then activated for a predetermined time after the message generator is activated for receiving messages from the central system. Bush neither shows nor suggests such a system. The examiner refers to column 9, lines 32-67 for showing a schedule for periodically activating a message generator according to a stored schedule. The portion of Bush referred to relates to data collector objects. As described by Bush, data collector objects collect data. Applicant sees nothing in Bush that suggests that the data collector objects can send messages. To the extent that Bush mentions that the data collector objects can operate on schedule, this falls short of applicant's claim which requires that a message generator for sending a registration message to a central system be periodically activated according to a stored schedule. The data collector objects are not message generators and there is no suggestion that they send registrations messages let alone registration messages that include a unique identifier.

The claim also requires a receiver activated for a predetermined time after the generator is activated for receiving messages from the central system. This is important for the reason discussed above. The examiner refers to column 8, lines 4-15 for this teaching. The passage referred to describes a technique called Heart Beating which is said to ensure that WMI temporary event consumers are reregistered when WMI is stopped but says nothing about applicant's claimed receiver activated for a predetermined time after a message

17

generator is activated for receiving messages from a central system. In fact, Bush seems to work differently. As Bush suggests in line 11, Heart Beating can alternatively be accomplished by having a single machine proxy for several other machines and check some known property every few minutes. If the machine cannot be reached to get the property then a network or other problem is possible. Applicant submits that this is exactly the problem that the claimed invention overcomes. It isn't necessary for a machine to check every few minutes to see if another machine is reachable. When the message generator sends the registration message to the central system it knows that it will be able to make a connection. By activating the receiver for a predetermined time after the message generator is activated it knows that it can receive messages from the central system because a temporary two-way communications channel has been created by sending the message. This is a clear advantage over the method described by Bush.

With regard to claim 13, applicant relies not on storing the schedule in memory but upon the limitation that the receiver receives a schedule from the central system. The examiner points to column 9, lines 32-57 of Bush but applicant sees no suggestion in the portion of Bush referred to to send a schedule from a central system to a remote machine as claimed.

With regard to claim 14, the schedule is sent from a central system in response to a registration message. The examiner refers to column 9, lines 32-39 and column 10, lines 46 through column 11, line 3. The examiner has not identified and applicant finds nothing in these sections to suggest sending a registration message or to receiving a schedule in response to the registration message.

18

With regard to claim 15, the claim requires that the remote machine is a gateway device that provides protocol or address translation to further machines. The examiner points to column 6, lines 25-43 but applicant sees no mention of providing address translation as required by the claim.

Claim 16 requires that the gateway device maintains the schedule and interacts with further machines as required to satisfy the schedule. This is a special case of applicant's invention wherein one of the remote machines acts as a gateway for further remote machines. The examiner refers to column 6, lines 25-43 of Bush for this teaching but applicant finds nothing like this in the referenced portion of Bush. Bush certainly says nothing about having a machine act as a gateway for a further machine or having the gateway machine maintain a schedule.

As to claim 17, applicant relies on the same differences as set forth in regard to claim 10 but notes that nothing in Bush mentions a firewall that prevents incoming connections to a machine. Moreover, claim 17 requires a listener for receiving a schedule from a central system which is not described in Bush and for periodically activating the message generator according to the stored schedule for creating a temporary two-way connection to a central system which is not described in Bush. While applicant agrees that TCP/IP connections are, or at least may be, two-way connections, the claim of course requires much more than this none of which is found in Bush.

Applicant doesn't rely separately on the limitations of claim 18.

With regard to claims 20 and 21, applicant repeats the distinctions drawn with respect to claim 10.

With respect to claim 22, the claim requires queuing one or more request messages on the server, logging the one or more request messages on the server, sending a polling message from the asset to the server, sending one of the one or more requests message to the asset in response to the polling message, sending a responsive message from the asset to the server, receiving the responsive message at the server and reconciling the responsive message with the logs request; and continuing to send request messages to the asset until the queue is empty. This claim implements a method of sending one or more messages to an asset that cannot be reached directly from the server. The examiner refers to column 11 of Bush for teaching these steps.

At Column 11, lines 23-32 Bush describes a polling operation comprising a timer activated every so many seconds with a minimum collection interval such as not less than a section during which the agent moves through its data collector instances and determines which ones need data collected therefore. There is no suggestion in Bush that this data collection activity includes any request messages or that even if the data collector instances are considered to be messages which applicant does not concede, that they are ever sent to an asset as required by the claim. It appears that the data collector instances simply acquire data on a schedule and compare the data to a threshold. It also appears that the data collector instances are simply executed on a schedule rather than being executed in response to a polling message as required by claim 22.

A general problem with the Bush reference is that Bush uses different terms from the terms used in applicant's claims and it is not clear which of the elements of Bush the examiner is calling the server and which elements he is

20

calling the device or asset as the terms are used by applicant. In some cases applicant believes that the examiner is reversing the Bush elements that he claims corresponds to applicant's claim limitations.

With respect to logging one or more request messages on the server, the examiner refers to column 11, lines 42-50 but nothing in that section of Bush shows or suggests the claim limitation. Bush refers to an Event Log 114 (this is wrong since the element labeled 114 is an actions provider as shown in figure 3) but in any case the log only records messages created in response to error thresholds being violated, not request messages as required by the claim. Further, the Event Log of Bush is not located on a server as required by the claim but on the machine being managed as shown in figure 3.

With regard to the limitation in claim 22 requiring sending a polling message from the asset to the server, the examiner relies on column 11, lines 4-14 but the polling referred to in this section is data collection not a request from an asset to a server for receiving a request message. Column 11, lines 25-28 already discussed, describes this in more detail.

The claim requires receiving the responsive message at the server and reconciling the responsive message with the log request. The examiner points to column 11, lines 12-14 but this section refers to something completely different namely inhibiting sending another request for data if the previous request has not yet been satisfied.

The claim also requires continuing to send request messages to the asset until the queue is empty. The examiner refers to column 12, lines 16-23 but this portion of Bush describes pulling events out of the event log 134 which it

will be recalled stores exceptions not request messages. Accordingly, Bush doesn't show or suggest sending request messages to the asset until the queue is empty.

With respect to claim 23, the claim requires that the step of sending a polling message comprises sending polling messages at pre-determined intervals. The examiner points to column 11, lines 23-25 of Bush but this portion of Bush relates to data collection not sending polling messages from an asset to a server.

Claim 24 requires the steps of detecting a fault at the asset and sending one or more polling messages to the server in response to the fault. The examiner points to column 12, lines 8-23 of Bush but Bush relates to something quite different. The designated portion of Bush describes what happens if the agent cannot process the necessary work load for each of its polling intervals and gets behind. As an example, there may be too many events being sent to the agent for it to handle in which case informational messages will be generated to alert the operator. Initially, this paragraph points out perhaps the most important distinction between Bush and applicant's invention, namely that events can be sent to the agent directly which is only possible if the agent is not located behind a fire wall. This is the very problem that applicant seeks to address. In any case, the section doesn't describe polling in response to a fault condition but simply sending events to the agent. The remainder of this section describes how the event log, which it will be recalled stores errors not messages, can be used to generate new events. None of this suggests detecting a fault at the asset and sending a polling message to a server in response to detecting the fault.

With regard to claim 25, the claim requires that the step of sending one or more polling messages comprises sending one or more polling messages at a second interval shorter than the predetermined interval. The examiner points to column 11, lines 23-25 which mentions a polling which as already described is not polling for request messages but polling for data, and furthermore doesn't appear to suggest polling at different intervals as the examiner suggests but rather a polling every so many seconds with a minimum collection interval possible such as not less than 1 second. This fails to describe or suggest a second interval shorter than a pre-determined interval.

With regard to claim 26, the claim requires that the second predetermined interval is set by the server. The examiner refers to column 11, lines 23-28 but nothing in this section suggests that there even is a second interval or that any interval is set by the server. Rather, it appears that the management client sets the interval and even at this, as already discussed, the polling in Bush is data collection that is not event driven while the claim requires collecting previously stored request messages for various operations.

With regard to claim 27, the claim requires that the server sends one or more queued messages to an asset in response to any message from the asset received from the server. The examiner points to column 12, lines 16-23 of Bush for this teaching. First of all, as discussed above, the events that are sent when the console first attaches or wants to see historical data are not request messages and second, the events are not sent in response to a message from the asset received by a server. In fact, if anything the process described in Bush appears to be the reverse of this.

With respect to claim 28 the claim requires that the server sends an indication of a queued message to an asset in response to various messages from the asset received by the server. Furthermore, the examiner slightly misreads claim 28 which requires that the server sends an _indication_ of a queued message to the asset in response to various messages from the asset received by the server. This allows the server to let the asset know that there are messages queued when the asset and server are communicating with respect to other messages. Bush discusses nothing like this.

With respect to claim 29, the claim requires that the message from the server includes a request for establishing an interactive session and a responsive message from the asset establishes an open connection through which subsequent messages are sent. This claim highlights the ability of the claimed invention to establish two-way connections through firewalls where a server cannot directly contact an asset. It can be easily seen that Bush does not teach this. The examiner points to column 12, lines 16-23 but nothing in the portion of Bush referred to suggests otherwise. Bush doesn't mention interactive sessions nor does he mention open connections. He doesn't mention requests for establishing an interactive session and he doesn't mention responsive messages. Accordingly, Bush fails to teach the subject matter of claim 29.

With respect to claim 30, applicant relies on the distinctions already made with respect to claims 15 and 16.

Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as unpatentable over Bush in view of Tabbara. Claim 11 requires a receiver for receiving an acknowledgement of the registration message and storing the token indicating

24

that the machine is registered. The examiner refers to paragraphs 89 and 90 of Tabbara. Applicant relies on the distinctions between Tabbara and the invention as set forth in claim 10, already discussed. In addition, Tabbara specifically provides that the authentication process can occur multiple times during operation of a node allowing the management devices for one or more ownership domains to change over time. This appears to be in direct contradiction to claim 11 which provides for storing a token and to claim 12 which further provides for inhibiting the sending of subsequent registration messages in response to the token. To the extent that Tabbara mentions a random token he is talking about a token used in public key cryptography not a method of recording that a machine has been registered.

Each of the matters raised in the office action having been addressed, reconsideration and favorable action are requested.

Respectfully submitted,

Dated: September 26, 2996

Stephen B. Salai, Registration No. 26,990
HARTER, SECREST & EMERY LLP
1600 Bausch & Lomb Place
Rochester, New York 4604
Telephone: 585-232-6500
Fax: 585-232-2152